CYBER ATTACKS ON NUCLEAR FACILITIES AND NUCLEAR RESPONSES TO CYBER ATTACKS IN INTERNATIONAL LAW

Nina Decoularé-Delafontaine

December 17, 2015

INTRODUCTION, RESEARCH QUESTION AND STRUCTURE

No sphere escapes to cyber threat, not even the most secured ones like nuclear facilities. In 2010, a complex and destructive worm called Stuxnet spread via a worker's USB stick into Iran's nuclear infrastructures in the city of Natanz. A fifth of Iran's uranium enrichment centrifuges were destroyed. This worm, designed and released by the U.S. and Israel, helped delay Tehran's potential ability to allegedly make its first nuclear weapon.[1] This case shows that a determined hacker (most likely with help from an insider when computers and networks are not connected to the Internet) could breach any security settings.[2] This Stuxnet episode for the first time really brought forward the question of the links between nuclear capacity and cyber capacity.

Not the assumption, but the realization that cyber capabilities will grow across the world has led many political analysts not to wonder *if* other states could gather enough capacity to deal critical cyber blows to physical infrastructure (including defense infrastructure), but rather *what* can be done to prevent them of doing so *when* they have the capacity.[3] In the U.S. as well as in other

[1] William J. Broad, John Markoff and David E. Sanger, *Israeli Test on Worm Called Crucial in Iran Nuclear Delay*, 01/15/2011, http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html?_r=0

[2] Pitz Samantha, *Cyber Vulnerabilities of Nuclear Weapons Are a Real National Security Threat*, 06/30/2015, http://nukesofhazardblog.com/cyber-vulnerabilities-of-nuclear-weapons-are-a-real-national-security-threat/

[3] Timothy Farnsworth, *Is there a place for nuclear deterrence in cyberspace?* 05/20/2013, http://armscontrolnow.org/2013/05/30/is-there-a-place-for-nuclear-deterrence-in-cyberspace/

parts of the world, various political figures in leading positions have compared the potential of a cyber attack to that of a nuclear attack.[4] The policy of deterrence will indeed inevitably be impacted by the rise of cyber operations. Whereas during the Cold War there was a theoretical belief that a strike on one's nuclear capability would result in mutually assured destruction, today's context is more complicated with non-violent cyber operations able to affect one's deterrence capacity and therefore potentially affect the balance of power.

If the nuclear deterrence system would be finally destabilized by use of a cyber attack against nuclear facilities, questions of *jus ad bellum* and *jus in bello* arise. In other words, the issue becomes of what the status of a cyber attack on nuclear infrastructure is, and of what responses are possible for the state that finds its nuclear deterrence potential affected by the cyber attack. These two questions are the research questions this paper will seek to answer. To assist answering these questions, the paper will use a fictional case to draw attention to some key points as to which there remains a lack of clarity within in international law.

This paper is divided in three parts. A first part focuses on the cyber attack and in itself treats three sub-questions related to cyber attacks in international law: (1) whether a cyber attack on nuclear infrastructure can constitute the prohibited use of force under UN Charter Article 2(4); (2) whether it can constitute an armed attack that triggers the right to self-defense under UN Charter Article 51; (3) how a cyber attack can be understood within international humanitarian law (IHL). Within all of these three sub-questions, one key consideration is (4) the problem of attribution, which will be discussed at the end of part 1 as an overarching problem. A second part of this paper focuses on the potential response of a nuclear state that finds itself threatened by a cyber attack on its nuclear infrastructure, and therefore focuses more on nuclear weapons law. This part

[4] Id.

will (1) discuss what countermeasures are possible if the initial attack is considered a prohibited use of force under UN Charter Article 2(4); (2) discuss the position of self-defense if the initial attack was considered an armed attack under UN Charter Article 51; (3) discuss the conundrum between requirements under IHL and the state practice of deterrence. Finally, (4) this part will offer a discussion of the elephant in the room with regards to a nuclear response: whether or not IHL constitutes jus cogens.

(0) FICTIONAL CASE

In order to enlighten the theoretical concepts used in international law with a practical point of view, this paper analyzes a fictitious case involving a cyber attack launched by a State against the nuclear infrastructure of another State. This paper does not consider the issue of cyber terrorism.

Ashmistry and Casiopeia, two big nuclear powers in the Bandy Ocean, entered into war 15 years ago in order to gain sovereignty over the Caroline Island situated halfway between their respective territories. This war lasted about 5 years and resulted in the independence of the East part of the island, today called Marvel State. Marvel State has since then maintained a close relationship, both political and economic, to Ashmistry, with which it shares the same religion.

Despite the independence of Marvel State, the relations between Ashmistry and Casiopeia have stayed really tense over the last 10 years regarding the status of the western part of the island generally referred to as Caroline West. Both states deployed troops in this region and increased their nuclear arsenal. This situation has gone for years and both states have at the same time improved their cyber capacity. The international community fears that this new competence could result in an attack and a hot war between Ashmistry and Casiopeia on the Caroline Island's territory.

As an attempt to resolve actual tensions peacefully, it was decided to organize a referendum in the Caroline West to determine whether a reunification process with Marvel's State should be introduced or whether the territory should become independent. Many people in favor of the independence hope it will be a first step towards the fusion with Casiopeia with which they share a common religion different from the majority one in Ashmistry and Marvel State. According to latest polls, a majority of votes would favor independence.

A week before the referendum was supposed to take place, nearly all of the Casiopeia's nuclear missiles on hair-trigger alert were simultaneously hit by a cyber attack launched by Marvel State. An emergency meeting with the Head of State and legal advisors was directly convened at the Ministry of Defense of Casiopeia. Even if Casiopeia could not determine where the attack came from, everybody was convinced that Ashmistry was responsible for it. Legal advisors were asked about which possibilities Casiopeia had at its disposal to respond to this attack.

(1) CYBER ATTACKS ON NUCLEAR INFRASTRUCTURE IN INTERNATIONAL LAW

1.1. Cyber Attacks as Prohibited Use of Force under UN Charter Article 2(4)

Can a cyber attack on nuclear infrastructure of another state constitute the use of force as understood under UN Charter Article 2(4)? In short, the answer is yes, even though there is no firm legal provision stipulating so. As well known, UN Charter Article 2(4) has been subjected to various interpretations. UN Charter Article 2(4) stipulates:

> *All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the purposes of the United Nations.*

Crucially, no formal international legal criteria have been developed about under which conditions an act can be defined as "use of force".[5] Therefore, to answer this question, reference need to be made to both case law and other authoritative interpretative sources. Across these sources, it is possible to observe two dominant approaches to determining whether a cyber attack can amount to the use of force prohibited by Article 2(4). A first approach is the so-called "instrument-based approach". This approach was dominant during the Cold War and simply focuses on the weapon used. This approach implies the use of military weapons. While appealing in pre-cyber years, the approach has been countered on many occasions since the end of the Cold War. There are textual arguments that refer to the difference in language between Article 4(2) and Article 51, stressing that Article 4(2) indeed does not explicitly refer to arms but to force. More importantly, the instrument-based approach has been rejected by the ICJ in its 1996 opinion on the legality of the threat or use of nuclear weapons. Indeed, the ICJ pointed out that article 2(4) "do[es] not refer to specific weapons [but] appl[ies] to any use of force, regardless of the weapons employed. The Charter neither expressly prohibits, not permits, the use of any specific weapon, including nuclear weapons."[6]

A second approach is the effects-based approach, which is now supported by more legal scholars and case law. This approach is also called the equivalence-based approach and stipulates that an attack constitutes a prohibited use of force if the effects produced are equivalent to those produced by conventional weapons. The real question in this case is whether the effect constitutes the same type of coercion, as the use of conventional military means would have done.[7] This is

[5] Jason Thelen, *Applying international law to cyber warfare*, 2014, presented at the RSA Conference 2014, Feburary 24-28, Moscone Center, San Francisco, http://www.rsaconference.com/writable/presentations/file_upload/law-f03a-applying-international-law-to-cyber-warfare.pdf

[6] Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons,* ICJ, 07/08/1996, para 39.

[7] Matthew Waxman "cyber attacks as "force" under UN Charter Article 2(4)" in International Law Studies Volume 87, Raul Pedrozo and Daria Wollschlaeger (Eds) *International Law and the Changing Character of War*, p44-46.

not an easy question, as there are many types of coercion. The drafting history of the UN Charter demonstrates that economic coercion was taken out of the scope of Article 2(4). Cyber operations that intend to economically coerce are therefore not considered prohibited uses of force.[8]

This is however short of saying that cyber operations cannot be considered uses of force. Rather, under the effects-based approach, many scholars and even states now acknowledge that cyber attacks can certainly constitute the use of force.[9] A prominent scholar elaborating early on this approach in the case of cyber attacks was Michael Schmitt. He developed a range of assessment factors to determine whether a cyber act constitutes the use of force.[10] These factors were then further developed by a group of legal experts who developed the Tallinn Manual.

The Tallinn Manual is the result of a three-year research project in which twenty international law experts, the so-called International Group of Experts, provided an overview and potential interpretations of the International Law Applicable to Cyber Warfare. Michael Schmitt led the project, which was executed with the support of the NATO Cooperative Cyber Defense Centre of Excellence (NATO CCD COE). The analysis was finally written down in the Tallinn Manual.[11] This text, however, does not constitute the codification of any rules. It merely brings together the analyses of a group of legal experts acting in their individual capacity. The strength of the Manual lies in the concluding principles that reflect consensus among all legal experts. These concluding

---

[8] Michael Schmitt, "Cyber operations in international law: the use of force, collective security, self-defense and armed conflicts" 2010 in *Proceedings of a Workshop on Deterring cyberattacks,* p155.

[9] Matthew Waxman "cyber attacks as "force" under UN Charter Article 2(4)" in International Law Studies Volume 87, Raul Pedrozo and Daria Wollschlaeger (Eds) *International Law and the Changing Character of War*, p47

[10] Jason Thelen, *Applying international law to cyber warfare*, 2014, presented at the RSA Conference 2014, Feburary 24-28, Moscone Center, San Francisco, http://www.rsaconference.com/writable/presentations/file_upload/law-f03a-applying-international-law-to-cyber-warfare.pdf

[11] Liis Vihul, *The Tallinn Manual on the International Law applicable to Cyber Warfare,* 04/15/2013, http://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/

principles, again, do not have the force of law, but they do indicate the potential existence of an authoritative scholarly source on the application of key norms of *jus ad bellum* and *jus in bello* to cyber operations. They have also withstood the test of time in state practice so far.[12]

The Tallinn Manual, in its Rule 11 sets forward the argumentation for an approach to identify the use of force that focuses on scale and effects:

> *A cyber operation constitutes a use of force when its scale and effects are comparable to non-cyber operations rising to the level of a use of force.*[13]

This rule was inspired by the doctrine of the ICJ in its Nicaragua Judgment, where the ICJ suggested that scale and effects ought to be used to identify whether an act constitutes an armed attack.[14] To assess whether a cyber attack should be regarded as a use of force, the Tallinn Manual further stipulates eight not formal legal criteria. Assessing these criteria make it clear that when relying on the Tallinn Manual, a cyber attack on nuclear infrastructure could very well constitute prohibited use of force.

- *Severity:* The scope, duration and intensity of the consequences need to be taken into account. An act resulting in physical harm to individuals or property will qualify as a use of force.
- *Immediacy*: A cyber operations is more likely to be considered as a use of force if it has immediate consequences. In this case indeed, States have less opportunity to seek peaceful and less harmful accommodation.

---

[12] Michael Schmitt, "Cyber operations in international law: the use of force, collective security, self-defense and armed conflicts" 2010 in *Proceedings of a Workshop on Deterring cyberattacks,* p156.

[13] Tallinn Manual on The International Law Applicable to Cyber Warfare, 2013, Cambridge University press, Rule 11, p45.

[14] ICJ, Judgment, *Military and Paramilitary Activities in and against Nicaragua,* 06/27/1986, para 195.

- *Directness:* This factor examines the chain of causation. In armed actions indeed, cause and effect are closely related.
- *Invasiveness:* "This refers to the degree to which cyber operations intrude into the target State or its cyber systems contrary to the interests of that State."
- *Measurability of effects:* A cyber operation is more likely to be characterized as a use of force if its set of consequences is quantifiable and identifiable.
- *Military character:* "A nexus between the cyber operation in question and military operations heightens the likelihood of characterization as a use of force."
- *State involvement:* "The clearer and closer a nexus between a State and cyber operations, the more likely it is that other States will characterize them as uses of force by that State."
- *Presumptive legacy:* An act not prohibited by law is presumptively permitted. For instance, international law does not prohibit propaganda, psychological operations, espionage or mere economic pressure. The acts falling into these categories are less likely to be considered by States as use of force.

In conclusion, cyber operations against nuclear infrastructure can be considered as prohibited use of force, provided that they together satisfy a group of conditions that is not yet developed in case law, but is highly regarded in legal scholarly literature. According to Schmidt, the threat or use of cyber operations against another state to coerce that state to cede territory would constitute the use of force. Crucial in this regard is the coercive intention of the originating state.[15]

A practical scenario in which a cyber attack on one's nuclear infrastructure constitutes the prohibited use of force but is short of an armed attack is difficult to conceive. However, it does

[15] Michael Schmitt, "Cyber operations in international law: the use of force, collective security, self-defense and armed conflicts" 2010 in *Proceedings of a Workshop on Deterring cyberattacks,* p153.

not appear impossible. Before discussing the difference, however, it seems appropriate to analyze cyber attacks on nuclear infrastructure as potential armed attacks under UN Charter Article 51.

1.2. Cyber Attack as Armed Attacks under UN Charter Article 51

Can a cyber attack on nuclear infrastructure of another state constitute an armed attack as understood under UN Charter Article 51? In short, the answer is yes, even though there is no firm legal provision stipulating so.

All armed attacks are uses of force but not all uses of force are armed attacks. This distinction between use of force and armed attack is important. Only an armed attack can allow legal self-defense with forceful means. The use of force that is not an armed attack can never, in the absence of UN Security Council action under Chapter VII, allow the targeted state to resort to a forceful response (*vide infra*). UN Charter Article 51 reads:

> *Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security.*

The general language in Article 51 begs the question of what an armed attack means and what exactly the difference with use of force is. This is not nearly as straightforward as it may seem. For example, in the wake of the ICJ Nicaragua Judgment, the position of the US was that the unlawful use of force constitutes an armed attack, which opens the possibility of forceful self-defense.[16]

[16] Abraham Sofaer, "International Law and the Use of Force" 1988 in *The National Interest,* no13, pp53-64.

As far as international case law goes, the ICJ has put forward, as mentioned above, the scale and effects approach. It did so in its Nicaragua Judgment, albeit without specifying how exactly to distinguish between use of force and armed attack. As mentioned, the Tallinn Manual has taken over this scales and effects approach to determine when cyber operations can amount to the prohibited use of force. Awkwardly yet logically given that the scales and effects approach was actually established by the ICJ in the context of "armed attack", the Tallinn Manual uses the exact same scales and effects standard with the same eight assessment factors to explore the existence of a cyber operation as an armed attack.

The International Group of Experts clearly remained confused, as most scholars, given the lack of clarity in either international legal rules or international case law. As indicated, there is somewhat of an ICJ case law based understanding that the standard to call something an armed attack is recognized as more stringent.[17] Indeed, the importance of the concept "armed attack" is that it explicitly refers to "armed", while "use of force" does not, and has been interpreted more broadly as such. Rather, an armed attack implies consequences of the action in the range of deaths or destruction of infrastructure.[18]

The element of destruction indeed appears central in many scholars' analyses.[19] Also in the Tallinn Manual, this element takes up a central role. That a cyber attack can constitute an armed attack is not in doubt. Consequent to the ICJ Nuclear Weapons Advisory Opinion, it is not the means of attack that matter.[20] A frequently drawn analogy is the use of biological or chemical weapons, which are also not classified as kinetic weapons but whose use can in no doubt

[17] Michael Schmitt, "Cyber operations in international law: the use of force, collective security, self-defense and armed conflicts" 2010 in *Proceedings of a Workshop on Deterring cyberattacks,* p163.

[18] Id.

[19] Nicholas Tsagourias and Russel Buchan, Research Handbook on International Law and Cyberspace, 2015, p122-123.

[20] ICJ, Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons,* 07/08/1996, para 39.

constitute an armed attack given their destructive consequence. In this regard, the International Group of Experts agreed that "any use of force that injures or kills persons or damages or destroys property would satisfy the scale and effects requirement" and thus constitute an armed attack.[21] Not constituting an armed attack includes "cyber intelligence gathering and cyber theft, as well as cyber operations that involve brief or periodic interruption of non-essential cyber services".[22]

As to the scale of destruction, it should finally be noted that the (elusive) benchmark is not of a quantitative but rather a qualitative scale. As Schmidt has pointed out well, in the Oil Platforms Case, the ICJ even acknowledged that the destruction of one single ship can constitute an armed attack. The author thereby convincingly confirms that under international law it appears that qualitative indicators are more important than quantitative ones.[23]

What is now the consequence of this difference for our fictional case involving a cyber attack on nuclear infrastructure? Within international law, the consequence is rather large. It is useful here to again assess the Stuxnet Operation against Iran. In this case, the virus inflicted by the United States and Israel to Iran's nuclear program clearly involved the destruction of physical property. It is estimated that in total about 1000 centrifuges were destroyed.[24] While there is clear physical destruction, the International Group of Experts did not agree whether this constituted an armed attack, and therefore whether it would be possible for Iran to exercise the right of self-defense.[25]

---

[21] Tallinn Manual on The International Law Applicable to Cyber Warfare, 2013, Cambridge University press, p56.

[22] Id.

[23] Michael Schmitt, "Cyber operations in international law: the use of force, collective security, self-defense and armed conflicts" 2010 in *Proceedings of a Workshop on Deterring cyberattacks,* p164.

[24] Andrew Foltz, "Stuxnet, Schmitt Analysis, and the Cyber "Use-of-Force Debate", 2012, in *JFQ* no 67, http://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-67/JFQ-67_40-48_Foltz.pdf

[25] Jason Thelen, *Applying international law to cyber warfare*, 2014, presented at the RSA Conference 2014, Feburary 24-28, Moscone Center, San Francisco,

In our fictional case of Casiopeia, the question would be as to what exactly is the scale and effect of the cyber attack on its nuclear infrastructure. Given the law above, one could wonder whether a cyber operation that does not lead to physical destruction of Casiopeia's nuclear *capacity* but rather temporarily incapacitates Casiopeia's nuclear *response* could plausibly be considered a prohibited use of force short of an armed attack. Indeed, even though some of the eight Tallinn assessment factors would be satisfied, the severity of the consequence of the operation would be limited in duration and no physical destruction would have taken place. In case the cyber operation did lead to the physical destruction of most of its nuclear capacity, the operation can indeed be more easily considered an armed attack. In this case, all of the eight above-described assessment factors are satisfied by the actual physical destruction of one's nuclear capacity: (1) it is severe in scope, duration and intensity; (2) it has immediate consequences for Casiopeia; (3) there is a direct link between the cyber attack and the effect; (4) it is highly invasive, particularly regarding the tension with Ashmistry and the upcoming referendum; (5) the effects are quantifiable and clear; (6) the cyber operation has a clear military character as it targets the nuclear defense infrastructure of Casiopeia; (7) state involvement appears clear, even though it remains short of confirmed; (8) the cyber operation, because of all of the above, is not presumed to be legal.

The assessment of these factors is clearly an exercise in understanding the political environment of the conflict. As we will see below, this is also a key consideration in determining attribution. In real life applications, the Stuxnet episode clearly shows how international politics and international law indeed cannot be treated in isolation of each other in the case of evolving cyber law. Simply put, state practice still demonstrates a phenomenal amount of caution to argue that a

---

http://www.rsaconference.com/writable/presentations/file_upload/law-f03a-applying-international-law-to-cyber-warfare.pdf; See also, Tallinn Manual on The International Law Applicable to Cyber Warfare, 2013, Cambridge University press, p58.

cyber operation constitutes the use of force or an armed attack. In the case of Stuxnet, Iran for example never publicly claimed that it constituted an armed attack.[26]

1.3. Application of International Humanitarian Law to Cyber Operations

To understand whether international humanitarian law applies, it is first required to determine whether an armed conflict exists. International law itself has no specific rules setting out what an armed conflict means. One authoritative interpretation often referred to[27] is the definition given by the International Criminal Tribunal for the Former Yugoslavia, in its Tadic decision:

> *On the basis of the foregoing, we find that armed conflict exists whenever there is a resort to armed force between States or protracted armed violence between governmental authorities and organized armed groups or between such groups within a State.*[28]

In the case of a cyber attack, what should thus first be assessed is whether this attack is part of a wider armed conflict and whether it can be attributed to a state in this conflict.[29] Generally, it has been long asserted that cyber attacks within an ongoing armed conflict are governed by international humanitarian law.[30] Gradually, states and international organizations have also explicitly recognized the applicability of international humanitarian law to cyber operations.[31]

---

[26] Gary Brown, Paul Walker and Anthony Bell III, "Military Cyberspace Operations" (2015), In Geoffrey Corn, Rachel VanLandingham and Shane Reeves, *U.S. Military Operations: Law, Policy, and Practice*., p138

[27] Nicholas Tsagourias and Russel Buchan, Research Handbook on International Law and Cyberspace, 2015, p. 121.

[28] Prosecutor v Dusko Tadic: Decision on the Defence motion for interlocutory appeal on jurisdiction, 10/02/1995, para 70.

[29] Nicholas Tsagourias and Russel Buchan, Research Handbook on International Law and Cyberspace, 2015, p. 122.

[30] Nils Melzer, *Cyberwarfare and international law,* 2011, UNIDIR Resources, p22-23.

[31] ICRC, *International humanitarian law and the challenges of contemporary armed conflicts,* Report prepared for the 32nd International Conference of the Red Cross and Red Crescent, Geneva, Switzerland, 8-10 December 2015.

Whether they can trigger an armed conflict is somewhat of a more complex question, to which no real answer exists as of yet. Here too, there exists an effects-based approach in which a cyber attack can have physical destruction as a consequence.[32] This destruction should be assessed in a broad way, in which the cyber attack needs to be found causal to the consequent destruction.[33]

Within international humanitarian law, destructive kinetic strikes are allowed, but only so if they are based on the status of the person or object they are targeted against. International humanitarian law specifies both a proportionality condition to destructive attacks, as well as the precautionary principle applied to the protection of civilians. Simply said, attacks and counter-attacks can target combatants but not civilians.[34] This principle of distinction has been wholly incorporated in the Tallinn Manual in Rule 31: "The principle of distinction applies to cyber attacks", and Rule 32: "Prohibition on attacking civilians".[35]

So far, this paper has addressed critical issues such as the use of force, armed attacks and armed conflict. In assessing these notions, it was found that the effect of physical destruction is a key element in any legal analysis. Yet, the analysis so far, however, leaves us somewhat wondering whether a cyber attack on nuclear infrastructure that does not directly lead to casualties or a huge amount of physical destruction can actually qualify as an attack. To answer this question, a more thorough reading of international humanitarian law can be useful.

[32] Nils Melzer, *Cyberwarfare and international law,* 2011, UNIDIR Resources, p24.

[33] Nicholas Tsagourias and Russel Buchan, Research Handbook on International Law and Cyberspace, 2015, p123.

[34] Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I), 06/08/1977, Article 58 and 52.

[35] Tallinn Manual on The International Law Applicable to Cyber Warfare, 2013, Cambridge University press, Rule 31 and 32.

It must be noted that a firm answer in international case law does not yet exist. That said, Article 52(2) of Protocol I of 08 June 1977 to the 1949 Geneva Conventions, while discussing the protection of civilians from attacks, provides a legal basis of argumentation that attacks shifting the military balance of power can constitute attacks under International Humanitarian Law even if they do not lead to destruction. Article 52(2):

> *Attacks shall be limited strictly to military objectives. In so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage.*[36]

As mentioned in the above analysis, many scholars are more careful and argue that it is both necessary and sufficient that some type of physical destruction (casualties or infrastructure) is necessary for an attack to be considered. The violent effect is thus central. As Melzer convincingly argues, neither interpretation is wholly satisfactory. Melzer further indicates the use of specific concepts in the Geneva conventions that could point toward a broader understanding of attack. These concepts include "military operation" instead of "attack" in the rule of distinction, and the use of "hostilities" when discussing the status of a civilian becoming a combatant.[37]

Also in our hypothetical case of Casiopeia, it seems illogical to assume a grand difference between a cyber attack that neutralizes a nuclear capacity with or without physical destruction. Rather, the effect of a military shift of power would matter most in terms of actual effect. In the

[36] Protocol additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of victims of international armed conflicts (Protocol I), 06/08/1977, Article 52(2).

[37] Nils Melzer, *Cyberwarfare and international law,* 2011, UNIDIR Resources, p26-27.

case of self-defense or a counter-attack, the issue of temporality needs to be taken into account. In the unlikely yet theoretically plausible situation that a cyber attack does not lead to actual physical destruction but nonetheless takes out the nuclear response capacity of a state for the long-term, the effects are clearly different from a short term "bug". It is very easy to understand that "duration" of the severity is actually politically the central element when it comes to mutual nuclear deterrence, as it indeed offers a definite military advantage, in this case, to Ashmistry.

Therefore, it seems that a first criterion for calling a cyber attack on Casiopeia is set. A second criterion, the existence of an armed conflict, remains somewhat unclear. The Tadic Decision stipulated that protracted armed violence between governments can indicate the existence of an armed conflict. Without going into detail on the notion of "protracted armed violence" (which is beyond the scope of this paper), it is perfectly conceivable that the conflict between Casiopeia and Ashmistry, especially over Caroline West in which both parties deployed troops, could be considered a protracted armed conflict, particularly because they have entered into war 15 years ago which only ended partially with the independence of one part of the Island, Marvel State. It should be noted that the cyber attack in this case could be considered as an armed attack that reignites the protracted armed conflict. It could therefore indicate the re-application of IHL to the conflict between Casiopeia and Ashmistry. Finally, a third criterion is state attribution, which is discussed in the next section.

1.4. The Attribution Problem

When Estonia was hit by major cyber attacks in 2007, it was found that while most attacks originated in Russia, others appeared to have originated in 177 other countries.[38] This

[38] Michael Schmitt, "Cyber operations in international law: the use of force, collective security, self-defense and armed conflicts" 2010 in *Proceedings of a Workshop on Deterring cyberattacks,* p152.

demonstrates how difficult it can already be to pinpoint an attack to one country. Attribution is the key prerequisite to establish state responsibility, and the establishment of state responsibility is key (1) to determine whether a cyber operation constitutes a prohibited use of force or an armed attack that gives the right of self-defense to the targeted state under *jus in bellum*, and (2) to evaluate whether an armed conflict exists under *jus in bello*.

The question of attribution in the case of a cyber operation against a state's nuclear infrastructure is one coin with two sides. A first side deals with the question of the standard of attribution in case there is no full certainty about the involvement of the alleged responsible state. A second side deals with the question of the standard of attribution in case the responsible entity is certain, but the link between the responsible *entity* and the alleged responsible *state* is somewhat complicated. These two sides demonstrate that the key question of attribution is about how certain a targeted state must be to respond to the alleged state. There is no international law standard about this level of certainty.[39]

The attribution determination requires technical evaluation but also a wider determination by the targeted state under the standard of overall reasonableness.[40] To determine attribution under a standard of overall reasonableness includes the elaboration of the political relations between the targeted and responsible state, the respective cyber capacities, and so forth. What is important is that when a State decided to act in self-defense, the burden of proof is on that State, not the original perpetuator.

[39] Id. p168.

[40] Liis Vihul, *The Tallinn Manual on the International Law applicable to Cyber Warfare*, 04/15/2013, http://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/

Other than for a nuclear attack, in a cyber world that operates in a manner that allows for anonymity, the question of certainty about the degree of control by the alleged responsible state is central.[41] Ultimately, cyber and nuclear attacks are in this regard very different, as attribution is fairly straightforward in case of the latter. As the targeted state needs to prove attribution, it first needs to prove the degree of control.

As there is no strict standard, the degree of control question will inevitably be assessed on a case-to-case basis.[42] International case law has, however, pointed to a number of characteristics. In its Nicaragua Judgment, the ICJ discussed the degree of control, which is required to sufficiently prove attribution. The ICJ put forward a fairly strict standard where there has to be evidence that the State "directed or enforced the perpetration" and therefore had "effective control of the military and paramilitary operations in the course of which the alleged violations were committed".[43] The ICJ, in its Judgment on the Application of Genocide Prevention, reconfirmed this standard of effective control and explained again that to assess the relationship between the responsible entity and the alleged perpetrating State, it is important to "look beyond legal status alone, in order to grasp the reality of the relationship between the person taking action, and the State to which he is so closely attached as to appear to be nothing more than its agent".[44]

Conclusive evidence that a third entity is a mere agent of the alleged perpetrating state is also supported by the ILC Articles on State Responsibility, albeit the standard there appears somewhat lower. Article 8 of the ILC Articles on State Responsibility:

---

[41] Christopher Haley, *A theory of Cyber Deterrence,* 02/06/2013 in *Georgetown Journal of International Affairs,* http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/

[42] Michael Schmitt, "Cyber operations in international law: the use of force, collective security, self-defense and armed conflicts" 2010 in *Proceedings of a Workshop on Deterring cyberattacks,* p158.

[43] ICJ, Judgment, *Military and Paramilitary Activities in and against Nicaragua,* 06/27/1986, para 115.

[44] ICJ, Judgement, *Application of the Convention on the Prevention and Punishment of the Crime of Genocide,* 02/26/2007, para 392.

> *The conduct of a person or group of persons shall be considered an act of a State under international law if the person or group of persons is in fact acting on the instructions of, or under the direction or control of, that State in carrying out the conduct.*

The ILC Articles on State Responsibility give further specifications that are relevant to our case. First, Article 4 confirms that the acts of an organ of a state are to be attributed to that state. Article 7 serves as *lex specialis* to this rule by specifying that an act is attributed to the state "even if it exceeds its authority or contravenes instructions".[45] This implies that even when persons within their function in the state operate without a direct order, their acts remain attributed to the state.

As with regards to our case, Article 6 of the ILC Articles on State Responsibility is relevant:

> *The conduct of an organ placed at the disposal of a State by another State shall be considered an act of the former State under international law if the organ is acting in the exercise of elements of the governmental authority of the State at whose disposal it is placed.*

Relying on the drafting history of the UN Charter, which demonstrated that states did not consider economic coercion as an act constituting the use of force, the Tallinn Manual finds that funding third non-state members to execute a cyber attack is insufficient to acknowledge a cyber attack from another state. Rather, some type of training or more direct involvement needs to be proven.[46] Relying on the arguments given by the U.S. to launch attacks against Al Qaeda and the Taliban in Afghanistan, Schmidt discusses one potential standard of reasonableness that stipulates

[45] 2001 Articles on the Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10, Art. 4 and 7.

[46] Liis Vihul, *The Tallinn Manual on the International Law applicable to Cyber Warfare*, 04/25/2013, http://www.ejiltalk.org/the-tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/

that the state needs to have clear and compelling evidence identifying the likely responsible state.[47]

This, however, does not mean Marvel State is excused from its responsibility under international law. As the ICJ put forward in Corfu Channel, a State has the obligation to disallow acts that would breach the rights of other states but which take place from its territory.[48]

Governments can deny involvement by channeling their actions via third states or even non-state groups. That said, attribution is still plausible in the real world, even if this may mean investing in technological capacity to identify the responsible state.[49] In the Casiopeia-Ashmistry conflict, it appears that there was sufficient technological capability to identify Marvel Island as the territory from which the cyber attack was launched.

Given the endured conflict between Casiopeia and Ashmistry, in particular over Caroline West, and with the upcoming referendum, it seems entirely plausible that the responsible state is actually Ashmistry, who also maintains good relations with the Government of Marvel State. These political realities, as indicated by the ICJ in Nicaragua and Genocide Prevention, are important to satisfy attribution requirements. That said, this is far from suggesting that these arguments are sufficient to satisfy Casiopeia's burden of proof. Rather, from the case at hand, it seems more that there is insufficient proof of degree of control.

---

[47] Michael Schmitt, "Cyber operations in international law: the use of force, collective security, self-defense and armed conflicts" 2010 in *Proceedings of a Workshop on Deterring cyberattacks,* p168.

[48] ICJ, Judgment, *Corfu Channel,* 04/09/1949, p22.

[49] Christopher Haley, *A theory of Cyber Deterrence,* 06 February 2013 in *Georgetown Journal of International Affairs,* http://journal.georgetown.edu/a-theory-of-cyber-deterrence-christopher-haley/

First, Ashmistry has not claimed the attack. Second, the facts in the case at hand do not establish that here was effective control, and that either Marvel State or an individual within Marvel State was a mere agent of Ashmistry. The facts also do not seem to support the potential that the cyber attack was merely directed by Ashmistry. Rather, alternative hypotheses could be that Marvel State does not want the independence of Caroline West, which is believed to favor unification with Casiopeia in the medium-term. In this hypothetical case, it should finally be noted that two main indicative proofs are missing: (1) the fact that the degree of cyber technology to carry out such an attack was decisively only present in Ashmistry state; (2) a clearer connection of control between Ashmistry state and those who carried out the attack in Marvel State.

(2) NUCLEAR RESPONSES TO CYBER ATTACKS ON NUCLEAR INFRASTRUCTURE IN INTERNATIONAL LAW

It might almost seem absurd to think that a nuclear strike could be a lawful response to a cyber attack, even if that cyber attack was targeted at a State's nuclear capacity, which is arguably one of the, if not the, most important cornerstone of a State's national security. However, the greatest mistake one could make is not to not know what is true, but rather to assume he knows what is true but actually is not.

That the field of international politics is full of dynamic experiences that seem too absurd even for the most creative of minds should not require further elaboration. Even in the sensitive and potentially all-destructive case of the use of nuclear weapons, debates continue to emphasize potential use. This is, of course, reflective of the policy of deterrence. One example of reflection is the U.S. Defense Science Board, which has recommended that the use of nuclear weapons

should be maintained as a final deterrence possibility against cyber attacks.[50] The subsequent part will discuss the potential legality of such a potential response.

2.1. Response to the prohibited use of force: Counter-measures

A breach of the prohibition of use of force under UN Charter 2(4) can only give way to non-forceful counter-measures. This, however, can change if the use of force is subsequently recognized as an armed attack under which forceful self-defense is legally allowed (*vide infra*).

As far as counter-measures go, Article 49 of the ILC Articles on State Responsibility clearly indicate that the injured state may only take countermeasures against the responsible state "to induce that State to comply with its obligations".[51] Article 50(1)(a) further clarifies that countermeasures do not affect the "obligation to refrain from the threat or use of force as embodied in the Charter of the United Nations".[52]

Contrary to these two standards, some have argued that state practice has developed differently and that countermeasures are not only often used in a punitive way post hoc, but also that international law should be able to allow for limited forceful countermeasures. Most prevalent in this regard is the separate opinion of Judge Simma in the ICJ Oil Platform Case.[53] Both state practice and the opinio juris of certain judges question whether the strict standard within the ILC Articles on State Responsibility actually represent customary international law.

---

[50] Timothy Farnsworth, Is there a place for nuclear deterrence in cyberspace? 05/20/2013, http://armscontrolnow.org/2013/05/30/is-there-a-place-for-nuclear-deterrence-in-cyberspace/

[51] 2001 Articles on the Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10, Art. 49(1)

[52] 2001 Articles on the Responsibility of States for Internationally Wrongful Acts, UN Doc. A/56/10, Art 50(1)(A)

[53] Separate Opinion of Judge Simma, *Oil Platforms,* 11/06/2003, p333.

On the question whether countermeasures can include the use of force, Schmitt convincingly argues that the Simma approach for limited forceful actions is problematic for the complementary nature of UN Charter Articles 2(4) and 51, with only the latter allowing for forceful response. It seems therefore that it is generally supported that under international law right now, forceful responses remain governed under the self-defense scheme of Article 51.[54]

This clearly means that if a cyber attack against nuclear infrastructure only constitutes the use of force, but not an armed attack, a nuclear response can never be justified under international law. In addition to the prohibition of the use of force, the countermeasure's objective of dissuasion of the responsible state's behavior makes it even more difficult, as once the cyber attack has been executed, there is potentially no more ongoing action that needs to be dissuaded, even if the balance of power or strategic advantage might have shifted.

2.2. Response to an armed attack: Self-defense

If a cyber attack on a nuclear facility has been identified as an armed attack, the targeted state can resort to forceful self-defense. There are two legal criteria to be assessed in the case of self-defense, as confirmed in the ICJ Nicaragua Judgment: necessity and proportionality.[55] In its Nuclear Weapons Advisory Opinion, the ICJ confirmed that the existence of these conditions were part of customary international law.[56]

The necessity criterion specifies that only the use of force that is required to stop an ongoing attack is allowed. This does not mean the use of force needs to be sufficient. Rather, the use of

[54] Michael Schmitt, "Cyber operations in international law: the use of force, collective security, self-defense and armed conflicts" 2010 in *Proceedings of a Workshop on Deterring cyberattacks,* p160.

[55] ICJ, Judgment, *Military and Paramilitary Activities in and against Nicaragua,* 06/27/1986, para 194.

[56] ICJ, Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons,* 07/08/1996, para 41.

force can be part of a broader response. The key to necessity is the question whether there exist non-forceful responses that can have the same effect. In the ICJ Judgment on Oil Platforms, the Court was not satisfied with the necessity requirement, as the US had not previously tried to resolve the issue diplomatically.[57] If a measure is not necessary, the validity of self-defense disappears.[58]

Once the use of force is deemed necessary, the proportionality criterion asks the question of what level of force is allowed as a response. The proportionality here lies in what is needed for self-defense. It is not about being proportional with the initial attack. Cyber attacks can be responded to with kinetic force, as much as kinetic force can be responded to with a stronger act of kinetic force, as long as it is proportional to the effectiveness of the self-defense. One important aspect of the principle of necessity and proportionality is the nature of the target against which force is used in light of self-defense.[59]

In the U.S. it has been confirmed in the 2011 White House International Strategy for Cyberspace, as well as in a 2011 Department of Defense Cyber Report to Congress, that cyber attacks give the US the capability to respond using "cyber and/or kinetic capabilities", provided they are in line with the principle of proportionality and other international law. Whether or not a nuclear attack can actually be proportional to a cyber attack is unclear in legal terms. In terms of political legitimacy, however, opinions are starkly divided. According to some, a nuclear attack can never be proportional to a cyber attack.[60]

---

[57] ICJ, Judgment, *Oil Platforms,* 06 November 2003, para 76.

[58] Id., para 43.

[59] Id., para 74.

[60] Timothy Farnsworth, Is there a place for nuclear deterrence in cyberspace? 05/20/2013, http://armscontrolnow.org/2013/05/30/is-there-a-place-for-nuclear-deterrence-in-cyberspace/

In international law so far, the ICJ Advisory Opinion on the Threat or Use of Nuclear Weapons, however much an artful exhibition of diplomatic legal writing, might have left more scholars confused and divided than before. The Court decided that either in customary or conventional international law there is neither a specific authorization nor a universal prohibition on the threat or use of nuclear weapons.[61] In a close 7 to 7 vote, where the President's casting vote ultimately decided on its adoption, the Court finally declared:

> *However, in view of the current state of international law, and of the elements of fact at its disposal, the Court cannot conclude definitively whether the threat or use of nuclear weapons would be lawful or unlawful in an extreme circumstance of self-defence, in which the very survival of a State would be at stake.*[62]

This supports the view that it is possibly plausible that a nuclear response to a cyber attack is lawful if the survival of a State is at stake. In the hypothetical case of Casiopeia and Ashmistry, it should be indicated that the necessity requirement is not fulfilled. Even if Ashmistry would claim the cyber attack, the political environment shows that this is eventually linked to the referendum and ultimate status of the territory of Caroline West. In this case, the very survival of Casiopeia is indeed not a stake. Even if there is an expectation that given the successful referendum, Caroline West will join Casiopeia in the medium term, this is no sufficient basis to argue that the very survival of Casiopeia is at stake. Again, even if Ashmistry's intention is to pursue a war in Caroline West after a majority yes-vote for independence, this again does not necessitate the use of a nuclear response from Casiopeia.

Whether a potential nuclear response could satisfy the principle of proportionality, however, is discussed together with an analysis of international humanitarian law in the next section.

---

[61] ICJ, Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons,* 07/08/1996, para 105.
[62] Id.

2.3. The Conundrum between Requirements under International Humanitarian Law and the Policy of Deterrence

Ultimately, the potential for a nuclear response to a cyber attack on one's nuclear response capacity can be best understood as a conundrum between requirements under the proportionality rule (*vide supra)* and under international humanitarian law from one side and the state practice of deterrence from another.

As far as international humanitarian law goes, the Court, logically, confirmed the rule of distinction between civilians and combatants, as well as the rule that combatants should not be made to suffer unnecessarily. In this context, the Court subsequently emphasized with regard to nuclear weapons that "the use of such weapons in fact seems scarcely reconcilable with respect for such requirements".[63] The phrasing of this statement clearly indicates the carefulness on behalf of the Court. The Court concludes:

> *Accordingly, in view of the present state of international law viewed as a whole, as examined above by the Court, and of the elements of fact at its disposal, the Court is led to observe that it cannot reach a definitive conclusion as to the legality or illegality of the use of nuclear weapons by a State in an extreme circumstance of self-defense, in which its very survival would be at stake.*[64]

In Paragraph 96, the Court expressly refers to the state practice of deterrence.[65] Together with insufficient facts about the controllability of nuclear weapons and the ultimate right to self-defense, this practice of deterrence makes up what the Court refers to in Paragraph 97 as "the

[63] ICJ, Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons,* 07/08/1996, para 95.
[64] Id. para 97.
[65] Id. para 96.

present state of international law viewed as a whole". The reference to state practice of deterrence seems far from irrelevant, exactly because of what it implies in terms of state practice to achieve stability through mutually assured destruction.

A first, key question in international law is thus whether the use of a nuclear weapon can be proportional and whether it can respect the rule of distinction in IHL. The issue at stake is one of controllability, which, of course, immediately feels opposite to the deterrence doctrine of mutually assured destruction.

2.3.1. The potential effects of nuclear weapons: controllability versus deterrence

The discussion of the potential effects of nuclear weapons is generally starkly divided, and it was no difference in the proceedings related to the ICJ Advisory Opinion on the Threat or Use of Nuclear Weapons. From one side, there are those emphasizing the controllability of a certain type of nuclear weapon, in particular the low yield nuclear weapons. In hearings before the ICJ on controllability, John McNeill of the US Department of Defense, set out a technical argument that a certain use of nuclear weapons can be controlled as with regards to their effect. According to him, there is no scientific evidence that all nuclear weapons would "violate the principles of proportionality and discriminate use in all cases".[66] In its written statement, the United States confirmed such position by arguing that modern delivery systems are not inherently indiscriminate and can indeed target specific military objectives.[67] Particular reference in this regard is made to military technology known as low yield nuclear weapons that are intended to be

[66] ICJ, *Legality of the Threat or Use of Nuclear Weapons*, public sitting held on Wednesday 15 November 1995 in the case in Legality of the Use by a State of Nuclear Weapons in Armed Conflict and in Legality of the Threat or Use of Nuclear Weapons, p70-71.

[67] Written statement of the Government of the United States of America before the International Court of Justice on an Advisory Opinion on the Legality of the Threat or Use of Nuclear Weapons, 06/20/1995, p23.

more accurate and less severe. In its stance before the ICJ, the United States disregarded the idea that the use of any nuclear weapon would inevitably lead to nuclear war.[68]

From another side, some, and in particular Judge Weeramantry in his dissenting opinion, focused on all the potential indiscriminate effects of nuclear weapons related to damaging the environment, future generations, and civilian populations caused by nuclear winter, loss of life, medical effects of radiation, heat and blast, and so forth.[69] In another dissenting opinion, Judge Koroma echoed Weeramantry by arguing that according to him, not the circumstances (ultimate self-defense) but rather the characteristics of those weapons would imply that their use would with certainty violate international law.[70]

It needs be noted, however, that even though the Court ultimately decided that it had insufficient facts to determine whether the use of nuclear weapons would in any case by unlawful, it did find that those supporting the view that controllable use was possible had failed to set forward under which specific circumstances this would be the case, including for the so-called low yield tactical nuclear weapons.[71] Therefore it found that the threat or use of nuclear weapons would generally be against international humanitarian law.[72] Interestingly, however, the Court in its final decision fails to link its conclusion explicitly to the existence of low-yield nuclear weapons. In effect,

[68] Charles J. Moxley Jr, *Nuclear Weapons and International Law in the Post Cold War World,* Draft book as of 10.01.2015 provided in the context of class "Nuclear Weapons and International Law in the Post 9/11 World", Fordham University School of Law, Fall 2015, p162.

[69] Dissenting Opinion of Judge Weeramantry, *Legality of the Threat or Use of Nuclear Weapons*, ICJ, 07/08/1996, p450-470.

[70] Dissenting Opinion of Judge Kouroma, *Legality of the Threat or Use of Nuclear Weapons*, ICJ, 07/08/1996, p571.

[71] ICJ, Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons,* 07/08/1996, para 94.

[72] Id., para 105.

omitting this reference keeps open the question as to whether the threat or use of larger, strategic nuclear weapons remains potentially legal.[73]

Even though the Court did not explicitly refer to plausible lawfulness of low yield tactical nuclear weapons, its foregoing analysis and emphasis on controllability does tend toward a prohibition of high yield nuclear weapons. That said, the Court remained short of actually prohibiting their use. This absence can only be understood in line with its reference to the policy of deterrence. There is somewhat of a conundrum in this regard. While international humanitarian law prohibits indiscriminate weapons, many states do believe that a policy of mutually assured destruction offered some stability. The mere content of mutually assured destruction of course implies the presence of high yield nuclear weapons, hence the conundrum before the Court.

The question on the lawfulness of deterrence remains unsettled. The Court did not expressly recognize the lawfulness of deterrence. In their separate and dissenting opinions, the judges demonstrated a stark contrast in views. Some judges strongly supported the policy of deterrence as state practice, and even went as far as to suggest that it was legitimized by conventional and customary international law, and lawful in itself. Other judges, however, questioned the legal status of deterrence, going as far as to suggest that the concept of deterrence has no legal force.[74]

While controllability is at center stage with regards to legal questions of proportionality and indiscriminate use, the clear key question to which this analysis has been building up is the apparent stand off between IHL and the Court's right to ultimate self-defense.

---

[73] Charles J. Moxley Jr, *Nuclear Weapons and International Law in the Post Cold War World,* Draft book as of 10.01.2015 provided in the context of class "Nuclear Weapons and International Law in the Post 9/11 World", Fordham University School of Law, Fall 2015, p191.

[74] Id. p235-242.

2.3.2. The stand off between IHL and Ultimate Self-Defense

Overall, the Court's Advisory Opinion concluded strongly in favor of a restrictive understanding of the illegality of the use of nuclear weapons. This means that in most cases their threat or use would likely be illegal, except that for in some cases of ultimate self-defense, their threat or use *may* not be illegal.[75]

Discussing the Court' approach in its Advisory Opinion on Nuclear Weapons, Moxley points out that the legal structure is possibly suggestive that the right to self-defense potentially overrides international humanitarian law. According to Moxley, it is striking that the court appears close to finding a complete prohibition of the threat or use of nuclear weapons, to then step back from that in its conclusion that it is uncertain whether the threat or use would be unlawful in the case of ultimate self-defense for the state's survival.[76]

The reading of the Advisory Opinion supports this analysis. While in Paragraph 95, the Court discusses that the use of nuclear weapons seems scarcely reconcilable with the requirements within IHL, Paragraph 96 takes a step back by saying that "the Court cannot lose sight of the fundamental right of every State to survival, and thus its right to resort to self-defense".[77] Subsequently, in Paragraph 97, the Court offers its conclusion "in view of the present state of international law as a whole".[78] While in its previous paragraph (96), the Court did also refer to the state practice of deterrence, its line of reasoning remains strikingly strong on the element of self-defense.

---

[75] Id. p188.
[76] Id. p189.
[77] ICJ, Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons,* 8 July 1996, para 95-96.
[78] Id., para 97.

This awkward relationship between international humanitarian law and the right to self-defense might have been best described by Judge Fleischhauer as a "dichotomy" [79]. He further asserted that "there is no rule in international law according to which one of the conflicting principles would prevail over the other".[80] This question is somewhat ambiguous and other Judges have given a vastly different understanding. For example Judge Koroma, in his dissenting opinion, concluded firmly that "the right to self-defence is inherent and fundamental to all States. It exists within and not outside or above the law […] The right of self-defence is not a licence to use force; it is regulated by law and was never intended to threaten the security of other states".[81]

It can only be concluded that the key question on the interaction between the right to self-defense and humanitarian law remains at best unsettled and realistically problematic. There remains an utter lack of clarity as to whether the ultimate right to self-defense should be understood as one that can be exercises within the limits of international humanitarian law, or rather should be considered as a logical consequence of the theoretical presumption that "no system of law can obliged those subject to it to commit suicide".[82] This theoretical presumption and its implications seem at the heart of the evolution of international law generally, and will be discussed in the final section of this paper.

2.4. Away from the Conundrum: Fundamental IHL rules as jus cogens?

[79] Separate Opinion of Judge Fleischhauer, *Legality of the Threat or Use of Nuclear Weapons*, ICJ, 8 July 1996, p305.

[80] Id., p307.

[81] Dissenting Opinion of Judge Kouroma, *Legality of the Threat or Use of Nuclear Weapons*, ICJ, 8 July 1996, p338.

[82] Quote from Judge Shahabuddeen in understanding the issue before the Court and before arguing in his dissenting opinion that there is no self-defense exception to humanitarian law: Dissenting Opinion of Judge Shahabuddeen, *Legality of the Threat or Use of Nuclear Weapons*, ICJ, 07/08/1996, p427.

The problem at hand is a demonstration of the schizophrenic character of contemporary international law. From one side, it maintains a bilateral identity, in which the State is the ultimate subject for itself, and in which inter-state relations (read: international law) are written according to a bilateral understanding. Simply said, states ultimately care for their own interests and security, but can agree on rules that serve these objectives with (like-minded) other states. In international relations, this approach coincides with the realist assumption of anarchy among self-interested states that individually seek to remain in control of their alliances that can serve their own survival or interests more broadly. In the eye of the realist, there is no such thing as an international community.

From another side, international law showcases an advanced set of rules that can be understood as reflecting community norms, intended to protect the international community of states and even, ultimately, the individual human being. In international relations, this approach coincides more with a constructivist approach that emphasized that a voluntary, partial release of sovereignty caused by joint beliefs such as justice opens a path to a real international community where the human regains centrality.

It is not difficult to understand how this schizophrenia practically plays out in the question on the threat or use of nuclear weapons, and even more so when a nuclear response capacity is threatened. As mentioned, mutually assured destruction relies on a state-based approach to security. Central here is a self-centered negative rationale to the stability of international relations. This stands in stark contrast with the community-based approach of international humanitarian law, which relies on a positive rationale: shared beliefs that an international community exists and that it can be strengthened to achieve international peace and security.

States, at times of severe crisis, became aware of the necessity of community norms. It is for this reason that international humanitarian law was developed. At the same time, it is the reason why the International Law Commission received the mandate from the UN General Assembly to codify international law, including the issue of state responsibility.[83] The ILC subsequently achieved success in codifying the existence of *jus cogens*.[84]

There however remains a grand debate on what exactly constitutes *jus cogens*. This debate is again caused by the dichotomy of approaches described above. Such a dichotomy ultimately endangers these international rules in general and the development of an international community in particular given contemporary challenges in international relations where states are more pushed toward safeguarding self-interest at the expense of firmly opting for the establishment of an international community.

Among international law scholars and judges of the ICJ, there is a substantial argumentation in favor of considering the most fundamental IHL rules as jus cogens. Rather ironically, and indicative of the diplomatic nature of its Advisory Opinion, the ICJ in Nuclear Weapons argued that it was unnecessary to decide on the status of the core humanitarian norms at hand.[85] Besides the dissenting opinion of Judge Weeramantry that unquestionably argued that core IHL norms are indeed *jus cogens*, also Judge Bedjaoui[86] and Judge Koroma[87] have pointed toward the *jus cogens*

[83] Proukaki, Elena Katselli. *The Problem of Enforcement in International Law: Countermeasures, the Non-Injured State and the Idea of International Community*, 2011, p56-58.

[84] Andrea Gattini, "A return ticket to 'Communitarisme', Please", 2002 in *The European Journal of International Law,* Vol13 No5, p1191.

[85] ICJ, Advisory Opinion, *Legality of the Threat or Use of Nuclear Weapons,* 07/08/1996, para 83.

[86] Declaration of President Bedjaoui, *Legality of the Threat or Use of Nuclear Weapons, ICJ, 8 July 1996,* para 21.

[87] Dissenting Opinion of Judge Koroma, *Legality of the Threat or Use of Nuclear Weapons,* ICJ, 07/08/1996, para 574.

nature of these core IHL rules. In addition, many legal scholars have at length argued convincingly that core IHL norms are indeed *jus cogens*.[88]

It can only be concluded that the Court chose a diplomatic option by easily discarding the necessity to decide on the exact status of core IHL norms. In fact, this was exactly needed for if it was found that they indeed constitute *jus cogens* or *jus cogens in statu nascendi,* then the conclusion may have been different. Indeed, in the case of *jus cogens,* there would have been emphasis on the fact that "no derogation is permitted"[89] from such norms as they are fundamental to the international community of states, and humanity.

That said, the politics of individual states appears to persist in trying to achieve certainty in international relations by relying on mutually assured destruction through the policy of deterrence. Eventually, the ICJ Advisory Opinion, consciously or not, allowed the conundrum to continue existing, making the belief in the existence of an actual international community only more elusive.

(3) CONCLUSION

From the above analysis, we can conclude that cyber attacks on the nuclear infrastructure of a State can, subject to a number of conditions, constitute the prohibited use of force, an armed attack that gives right to self-defense and an armed attack within the context of a protracted armed conflict under international humanitarian law. We do find that the international legal

[88] Vincent Chetail, "The contribution of the International Court of Justice to International Humanitarian Law", in Bernard et al (eds.), IRRC 235 (2003), p251.

[89] 1969 Vienna Convention on the Law of Treaties, Article 53.

standards of attribution may be stringent in the case of a cyber attack, as such attacks operate on a much more anonymous and hidden basis than the use of conventional weaponry. Whether or not a nuclear state can respond to such a cyber attack with a limited nuclear strike is more open for discussion. We conclude that a cyber attack that constitutes the use of force but falls short of being an armed attack can never be responded to with the use of force itself. If the cyber attack does constitute an armed attack, the rules governing self-defense and international humanitarian law appear difficult to appease with a nuclear strike. The main reason for this is the controllability of the effect of nuclear weapons. The existence of low yield nuclear weapons whose effects can be carefully predicted remains debated without conclusive evidence.

More important in international law, however, seems to be the impossibility to marry a policy of deterrence and mutually assured destruction, which ultimately relies on high yield weapons, with the requirements under international humanitarian law. The debate in front of the ICJ during its Advisory Opinion on the Threat or Use of Nuclear Weapons appears to have lost focus of the bigger picture: whether or not fundamental norms of international humanitarian law constitute *jus cogens*. In the end, the decision did very little but highlighting the conflict schizophrenic identity of international law when its state-centrist function clashes with its international community developing function.